**Practitioner's Docket No. NAI1P489/03.047.01** *PATENT*

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Igor Garrievich Muttik

Application No.: 10/755,450 Group No.: 2432
Filed: 01/13/2004 Examiner: Lanier, Benjamin E.
For: DETECTING MALICIOUS COMPUTER PROGRAM ACTIVITY USING EXTERNAL PROGRAM CALLS WITH DYNAMIC RULE SETS

**Mail Stop Appeal Briefs – Patents**
**Commissioner for Patents**
**P.O. Box 1450**
**Alexandria, VA 22313-1450**

**TRANSMITTAL OF APPEAL BRIEF**
**(PATENT APPLICATION--37 C.F.R. § 41.37)**

**1.** This brief is in furtherance of the Notice of Appeal, filed in this case on 06/17/2009.

**2.** STATUS OF APPLICANT

This application is on behalf of other than a small entity.

**3.** FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

| | |
|---|---|
| other than a small entity | $540.00 |
| **Appeal Brief fee due** | **$540.00** |

**4.** EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time, the fees for which are set out in 37 C.F.R. § 1.17(a)(1)-(4), for two months:

Fee: $490.00

5. TOTAL FEE DUE

The total fee due is:

| | |
|---|---|
| Appeal brief fee | $540.00 |
| Extension fee (if any) | $490.00 |
| **TOTAL FEE DUE** | **$1,030.00** |

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $1,030.00 to Deposit Account No. 50-1351 (Order No. NAI1P489).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P489).

Date: October 19, 2009

/KEVINZILKA/
Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

**PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| In re application of: | ) | |
| | ) | |
| Igor Garrievich Muttik | ) | Group Art Unit: 2432 |
| | ) | |
| Application No. 10/755,450 | ) | Examiner: Lanier, Benjamin E. |
| | ) | |
| Filed: 01/13/2004 | ) | Atty. Docket No.: |
| | ) | NAI1P489/03.047.01 |
| For: DETECTING MALICIOUS COMPUTER | ) | |
| PROGRAM ACTIVITY USING | ) | Date: 10/19/2009 |
| EXTERNAL PROGRAM CALLS WITH | ) | |
| DYNAMIC RULE SETS | ) | |
| | ) | |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on 06/17/2009.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

## I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

**II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))**

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, a prior appeal was noted on 01/31/2008 in the present application.

A Related Proceedings Appendix is appended hereto.

## III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

### A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55

### B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55
3. Claims allowed: None
4. Claims rejected: 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55
5. Claims cancelled: 2, 14, 19, 31, 36, 48, 53, and 54

### C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55

See additional status information in the Appendix of Claims.

**IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))**

As to the status of any amendment filed subsequent to final rejection, the Amendment submitted on 04/28/2008 was entered by the Examiner.

## V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1, 2, and 4 et al., a computer program product embodied on a tangible computer readable medium operable to detect malicious computer program activity is provided. The computer program product comprises logging code that is operable to log a stream of external program calls (e.g. see item 14 of Figure 2, etc.), and primary set identifying code that is operable to identify, within the stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules (e.g. see item 10 of Figures 1 and 4, etc.). Additionally, the computer program product comprises secondary set identifying code that is operable to identify, within the stream, at least one secondary set of one or more external program calls associated with the primary set of one or more external program calls, and modifying code that is operable to modify the set of rules (e.g. see item 10' of Figure 4, etc.) such that the at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than the primary set of the one or more external program calls.

Further, the computer program product comprises promoting code operable to determine whether the modified set of rules (e.g. see item 10' of Figure 4, etc.) decreases malicious network traffic, and to promote the modified set of rules from a temporary set to a permanent set if it is determined that the modified set of rules decreases the malicious network traffic, and additional promoting code operable to determine whether the modified set of rules slows malware propagation, and to promote the modified set of rules from the temporary set to the permanent set if it is determined that the modified set of rules slows the malware propagation. Further still, one of the at least one secondary set of one or more external program calls precedes the primary set of one or more external program calls within the stream of external program calls. Also, the set of rules is modified to include a new rule corresponding to the secondary set of one or more external program calls, the new rule thereafter being used in addition to other rules within the set of rules. See, for example, page 3, lines 5-15, page, 4, line 1, page 6, lines 4-12, and page 8, lines 28-30 et al.

With respect to a summary of Claim 18, as shown in Figures 1, 2, and 4 et al., a method of detecting malicious computer program activity is provided. In use, a stream of external program calls (e.g. see item 14 of Figure 2, etc.) is logged, and a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules (e.g. see item 10 of Figures 1 and 4, etc.) is identified within the stream of external program calls. Additionally, at least one secondary set of one or more external program calls associated with the primary set of one or more external program calls is identified within the stream, the set of rules is modified (e.g. see item 10' of Figure 4, etc.) such that the at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than the primary set of the one or more external program calls.

Further, it is determined whether the modified set of rules (e.g. see item 10' of Figure 4, etc.) decreases malicious network traffic, and the modified set of rules is promoted from a temporary set to a permanent set if it is determined that the modified set of rules decreases the malicious network traffic. Further still, it is determined whether the modified set of rules slows malware propagation, and the modified set of rules is promoted from the temporary set to the permanent set if it is determined that the modified set of rules slows the malware propagation. Also, one of the at least one secondary set of one or more external program calls precedes the primary set of one or more external program calls within the stream of external program calls, and the set of rules is modified to include a new rule corresponding to the secondary set of one or more external program calls, the new rule thereafter being used in addition to other rules within the set of rules. See, for example, page 3, lines 5-15, page, 4, line 1, page 6, lines 4-12, and page 8, lines 28-30 et al.

With respect to a summary of Claim 35, as shown in Figures 1, 2, and 4 et al., a data processing apparatus operable to detect malicious computer program activity is provided. In use, the data processing apparatus comprises logging logic operable to log a stream of external program calls (e.g. see item 14 of Figure 2, etc.), and primary set identifying logic operable to identify, within the stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules (e.g. see item 10 of Figures 1 and 4, etc.). Additionally, the data processing apparatus

comprises secondary set identifying logic operable to identify, within the stream, at least one secondary set of one or more external program calls associated with the primary set of one or more external program calls, and modifying logic operable to modify the set of rules (e.g. see item 10' of Figure 4, etc.) such that the at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than the primary set of the one or more external program calls.

Further, the data processing apparatus comprises promoting logic operable to determine whether the modified set of rules (e.g. see item 10' of Figure 4, etc.) decreases malicious network traffic, and to promote the modified set of rules from a temporary set to a permanent set if it is determined that the modified set of rules decreases the malicious network traffic, and additional promoting logic operable to determine whether the modified set of rules slows malware propagation, and to promote the modified set of rules from the temporary set to the permanent set if it is determined that the modified set of rules slows the malware propagation. Further still, one of the at least one secondary set of one or more external program calls precedes the primary set of one or more external program calls within the stream of external program calls. Also, the set of rules is modified to include a new rule corresponding to the secondary set of one or more external program calls, the new rule thereafter being used in addition to other rules within the set of rules. See, for example, page 3, lines 5-15, page, 4, line 1, page 6, lines 4-12, and page 8, lines 28-30 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has objected to the Specification as failing to provide proper antecedent basis for the claimed subject matter.

Issue # 2: The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

Issue # 3: The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, and 49-52 under 35 U.S.C. 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

**VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))**

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has objected to the Specification as failing to provide proper antecedent basis for the claimed subject matter.

Specifically, the Examiner has argued that "[t]he phrase 'computer readable medium,' is not found to have proper antecedent basis in the specification" and that "[i]n order to overcome the objection, an amendment to the specification is necessary constituting a non-exhaustive statement of what the phrase 'computer readable medium' would be as it would have been known… in order to verify that the term… could not be taken in the context of non-statutory subject matter."

Appellant respectfully disagrees and notes that in Claim 1, appellant specifically claims "[a] computer program product embodied on a tangible computer readable medium" (emphasis added), which is clearly statutory. Additionally, appellant respectfully directs the Examiner's attention to Page 11, lines 14-16 and 21-23 of appellant's specification, which discloses that "computer program instructions… may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210" and that a "computer program may be stored and distributed on a recording medium or dynamically downloaded to the general purpose computer 200" (emphasis added), which are clearly examples of tangible computer readable mediums. Therefore, appellant's claimed "tangible computer readable medium" is clearly supported by the Specification, as claimed.

Of course, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

Issue # 2:

The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement.

*Group #1: Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, 49-52, and 55*

Specifically, the Examiner has argued that "[t]he specification does not disclose how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation" and that "it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware."

Appellant respectfully disagrees. First, appellant's claimed "determining whether said modified set of rules decreases malicious network traffic" and "determining whether said modified set of rules slows malware propagation" (see this or similar, but not necessarily identical language in the independent claims) is sufficiently enabled on Page 6, lines 4-12 of appellant's specification. For example, such excerpt discloses that "after a modified set is transmitted to other computers some network sensors detect the effect (e.g., decrease of traffic) and send a 'positive' signal back" (Page 6, lines 9-11), which clearly teaches how to detect whether the modified set of rules decreases malicious network traffic or slows malware propagation, as noted by the Examiner.

Additionally, in response to the Examiner's allegation that "it is unclear how modified rules in one particular system has any effect on the amount of malicious traffic or the amount of propagated malware," appellant respectfully points to Page 3, lines 17-25 of appellant's specification, which discloses that "[a secondary set of ]external program calls logged in association with the primary set of external program calls known to correspond to malicious computer program activity may themselves subsequently be used as an indicator for malicious computer program activity," where "[t]he secondary sets of external program calls are 'tainted' by their association with the primary set of external program calls and the set of rules may be modified to be more sensitive to the secondary set of external program calls," and where "the set of rules associated with malicious computer program activity may be extended and the detection made potentially more sensitive, reliable and proactive" (emphasis added).

Therefore, in one embodiment, the modified set of rules may be more sensitive to additional external program calls, and may therefore be extended, resulting in more sensitive, reliable, and proactive detection, which may in turn decrease malicious network traffic and slow malware propagation. Again, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

Issue # 3:

The Examiner has rejected Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, and 49-52 under 35 U.S.C. 112, second paragraph, as failing to particularly point out and distinctly claim the subject matter which appellant regards as the invention.

*Group #1: Claims 1, 3-13, 15-18, 20-30, 32-35, 37-47, and 49-52*

Specifically, the Examiner has argued that "[t]he term 'more strongly associated' is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention."

Appellant respectfully disagrees. First, appellant respectfully notes that appellant specifically claims "modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (emphasis added - see this or similar, but not necessarily identical language in the independent claims). Therefore, appellant clearly claims that "said at least one secondary set… are more strongly associated with malicious computer program activity than said primary set" (emphasis added).

Additionally, appellant respectfully points to Page 4, lines 29-32 of appellant's specification, where it is disclosed that "a particularly convenient way of modifying the rule set [to] make it more sensitive to the secondary sets of external program calls is to increase the score values associated with such secondary sets of external program calls" (emphasis added). Additionally, Page 9, lines 21-26 of appellant's specification discloses "the generation of plurality of new rules

which serve to more strongly associate the secondary sets of external program calls with malicious activity," where "[t]he secondary sets themselves may not be sufficient to trigger the anti-malware response, but their score values are increased such that when they occur in combination with other detected behavioural characteristics an anti-malware response will now be triggered" (emphasis added). Therefore, in one embodiment, appellant's claimed "at least one secondary set of one or more external program calls" is "more strongly associated with malicious computer program activity" by "increas[ing] the score values associated with such secondary sets of external program calls" (emphasis added).

As a result, appellant's aforementioned claim language clearly is particularly pointed out and distinctly claimed. Again, it should be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

Also, appellant's claimed "modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls" (see this or similar, but not necessarily identical language in the independent claims) is purposefully drafted in a broad manner, and it would be unduly limiting for the Examiner to require appellant to specifically "provide a standard for ascertaining the requisite degree," as argued by the Examiner.

Additionally, the Examiner has argued that "it is unclear how modifying 'said set of rules' has any effect on a set of program calls that has already been logged, or the amount of malicious network traffic and malware propagation."

Appellant respectfully disagrees. First, appellant respectfully asserts that appellant's claims do not necessarily recite that a modified set of rules has an effect on a set of program calls that has already been logged, as suggested by the Examiner. For example, appellant claims "modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls…wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external

program calls, said new rule thereafter being used in addition to other rules within said set of rules" (see this or similar, but not necessarily identical language in the independent claims).

Second, appellant points to Page 8, lines 8-11 and 17-21, which disclose one exemplary embodiment in which "checking is performed... which includes within its functionality the logging of a stream of external program calls, the identification of a primary set of program instruction calls found to match a rule or set of rules within the rules 10 and corresponding to malicious computer program activity," where "results associated with a particular external program call may also be examined and form part of the rule comparisons performed... in determining whether a particular external program call or set of external program calls matches one of the rules for identifying malicious computer program activity" (emphasis added).

Therefore, in one embodiment, results associated with an external program call may form part of rule comparisons that are performed for purposes of identifying malicious computer program activity. Thus, as shown hereinabove, appellant's aforementioned claim language clearly is particularly pointed out and distinctly claimed. Also, it should again be noted that the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

**VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))**

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product embodied on a tangible computer readable medium operable to detect malicious computer program activity, comprising:

logging code operable to log a stream of external program calls;

primary set identifying code operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying code operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls;

modifying code operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls;

promoting code operable to determine whether said modified set of rules decreases malicious network traffic, and to promote said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules decreases said malicious network traffic; and

additional promoting code operable to determine whether said modified set of rules slows malware propagation, and to promote said modified set of rules from said temporary set to said permanent set if it is determined that said modified set of rules slows said malware propagation;

wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls;

wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

2. (Cancelled)

3. (Original) A computer program product as claimed in claim 1, wherein said external program calls are application program interface calls to an operating system.

4. (Original) A computer program product as claimed in claim 1, wherein each of said external program calls has one or more characteristics compared against said set of rules.

5. (Original) A computer program product as claimed in claim 4, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values;

and one or more returned results.

6. (Original) A computer program product as claimed in claim 1, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

7. (Previously Presented) A computer program product as claimed in claim 6, wherein score values within a set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity than said primary set of said one or more external program calls.

8. (Original) A computer program product as claimed in claim 1, wherein said set of rules include at least one of:

one or more pattern matching rules; and

one or more regular expression rules.

9. (Original) A computer program product as claimed in claim 1, wherein said set of rules are responsive to ordering of external program calls.

10. (Original) A computer program product as claimed in claim 1, wherein said modifying code dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

11. (Previously Presented) A computer program product as claimed in claim 1, wherein at least changes within said set of rules are transmitted to one or more remote computers such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

12. (Original) A computer program product as claimed in claim 1, wherein changes within said set of rules are transmitted to a rule supplier.

13. (Original) A computer program product as claimed in claim 1, wherein said stream of external program calls are logged following emulation of execution of a computer program.

14. (Cancelled)

15. (Original) A computer program product as claimed in claim 1, comprising starting point identifying code operable to identify a starting point of malicious computer program activity within said stream of external program calls.

16. (Original) A computer program product as claimed in claim 15, wherein said starting point corresponds to one of:

starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

17. (Original) A computer program product as claimed in claim 1, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.

18. (Previously Presented) A method of detecting malicious computer program activity, said method comprising the steps of:

logging a stream of external program calls;

identifying within said stream of external program calls a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

identifying within said stream at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls;

modifying said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls;

determining whether said modified set of rules decreases malicious network traffic, and promoting said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules decreases said malicious network traffic; and

determining whether said modified set of rules slows malware propagation, and promoting said modified set of rules from said temporary set to said permanent set if it is determined that said modified set of rules slows said malware propagation;

wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls;

wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

19. (Cancelled)

20. (Original) A method as claimed in claim 18, wherein said external program calls are application program interface calls to an operating system.

21. (Original) A method as claimed in claim 18, wherein each of said external program calls has one or more characteristics compared against said set of rules.

22. (Original) A method as claimed in claim 21, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values; and

one or more returned results.

23. (Original) A method as claimed in claim 18, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

24. (Previously Presented) A method as claimed in claim 23, wherein score values within a set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity than said primary set of said one or more external program calls.

25. (Previously Presented) A method as claimed in claim 18, wherein said set of rules include at least one of:

one or more pattern matching rules; and

one or more regular expression rules.

26. (Original) A method as claimed in claim 18, wherein said set of rules are responsive to ordering of external program calls.

27. (Original) A method as claimed in claim 18, wherein said step of modifying said set of rules dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

28. (Previously Presented) A method as claimed in claim 18, wherein at least changes within said set of rules are transmitted to one or more remote computers such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

29. (Original) A method as claimed in claim 18, wherein changes within said set of rules are transmitted to a rule supplier.

30. (Original) A method as claimed in claim 18, wherein said stream of external program calls are logged following emulation of execution of a computer program.

31. (Cancelled)

32. (Original) A method as claimed in claim 18, comprising identifying a starting point of malicious computer program activity within said stream of external program calls.

33. (Original) A method as claimed in claim 32, wherein said starting point corresponds to one of: starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

34. (Original) A method as claimed in claim 18, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.

35. (Previously Presented) A data processing apparatus operable to detect malicious computer program activity, said apparatus comprising:

logging logic operable to log a stream of external program calls;

primary set identifying logic operable to identify, within said stream of external program calls, a primary set of one or more external program calls matching one or more rules indicative of malicious computer program activity from among a set of rules;

secondary set identifying logic operable to identify, within said stream, at least one secondary set of one or more external program calls associated with said primary set of one or more external program calls;

modifying logic operable to modify said set of rules such that said at least one secondary set of one or more external program calls are more strongly associated with malicious computer program activity than said primary set of said one or more external program calls;

promoting logic operable to determine whether said modified set of rules decreases malicious network traffic, and to promote said modified set of rules from a temporary set to a permanent set if it is determined that said modified set of rules decreases said malicious network traffic; and

additional promoting logic operable to determine whether said modified set of rules slows malware propagation, and to promote said modified set of rules from said temporary set to said permanent set if it is determined that said modified set of rules slows said malware propagation;

wherein one of said at least one secondary set of one or more external program calls precedes said primary set of one or more external program calls within said stream of external program calls;

wherein said set of rules is modified to include a new rule corresponding to said secondary set of one or more external program calls, said new rule thereafter being used in addition to other rules within said set of rules.

36. (Cancelled)

37. (Original) An apparatus as claimed in claim 35, wherein said external program calls are application program interface calls to an operating system.

38. (Original) An apparatus as claimed in claim 35, wherein each of said external program calls has one or more characteristics compared against said set of rules.

39. (Original) An apparatus as claimed in claim 38, wherein said one or more characteristics include:

a call name;

a return address;

one or more parameter values; and

one or more returned results.

40. (Original) An apparatus as claimed in claim 35, wherein rules within said set of rules specify score values of external program calls having predetermined characteristics and a set of one or more external program calls is identified as corresponding to malicious computer program activity if said set of one or more external program calls has a combined score value exceeding a threshold level.

41. (Previously Presented) An apparatus as claimed in claim 40, wherein score values within a set of rules associated with said secondary set of one or more external program calls are increased to more strongly associate said secondary set of external program calls with malicious computer program activity than said primary set of said one or more external program calls.

42. (Original) An apparatus as claimed in claim 35, wherein said set of rules include at least one of:

one or more pattern matching rules; and

one or more regular expression rules.

43. (Original) An apparatus as claimed in claim 35, wherein said set of rules are responsive to ordering of external program calls.

44. (Original) An apparatus as claimed in claim 35 wherein said modifying logic dynamically adapts said set of rules in response to detected streams of external program calls performing malicious computer program activity.

45. (Previously Presented) An apparatus as claimed in claim 35, wherein at least changes within said set of rules are transmitted to one or more remote computers such that said one or more remote computers can use said modified set of rules without having to suffer said malicious computer program activity.

46. (Original) An apparatus as claimed in claim 35, wherein changes within said set of rules are transmitted to a rule supplier.

47. (Original) An apparatus as claimed in claim 35, wherein said stream of external program calls are logged following emulation of execution of a computer program.

48. (Cancelled)

49. (Original) An apparatus as claimed in claim 35, comprising starting point identifying logic operable to identify a starting point of malicious computer program activity within said stream of external program calls.

50. (Original) An apparatus as claimed in claim 49, wherein said starting point corresponds to one of: starting execution of a computer file; and

a switch of memory address region from which program instruction are executed.

51. (Original) An apparatus as claimed in claim 35, wherein said set of rules is subject to a validity check after modification to determine if said set of rules is more effectively detecting malicious computer program activity.

52. (Previously Presented) A computer program product as claimed in claim 1, further comprising applying high level rules to said modified set of rules, and promoting said modified set of rules from said temporary set to said permanent set based on the application of the high level rules to said modified set of rules.

53. (Cancelled)

54. (Cancelled)

55. (Previously Presented) A computer program product as claimed in claim 1, wherein one or more other rules are applied to said modified set of rules to determine if said modified set of rules is more effectively detecting malicious computer program activity after modification.

**IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))**

There is no such evidence.

## X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P489).

Respectfully submitted,

By: /KEVINZILKA/ Date: October 19, 2009
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660